

Amendments to the Claims:

This listing of claims replaces all prior versions and listings of claims in the application:

Listing of Claims:

1. (Currently Amended) A graphical user interface rendered on a display device the graphical user interface for configuring a new service detection process, the graphical user interface comprising:
 - a first field that depicts choices for entities to track in the network;
 - a second field that allows a system to track if the selected entity is providing or consuming a service;
 - a third field that depicts a range over which to track an entity selected in the first field; and
 - a fourth field to specify a severity for an alert generated if a new service is detected.
2. (Original) The graphical user interface of claim 1 wherein the fields are linguistically tied together on the interface to form a sentence that corresponds to a rule.
3. (Original) The graphical user interface of claim 1 further comprising:
a list of new service detection rules stored in the detection system.
4. (Original) The graphical user interface of claim 1 wherein the first field allows a user to specify entity to track as “a specific host”, “any host in a specific role”, “any host in a specific segment” or “any host.”
5. (Original) The graphical user interface of claim 1 wherein the third field specifies details for the extent of the comparison for the entity specified in the first field as “host”, “in its role”, “in its segment” or “anywhere” in the network.

6. (Original) The graphical user interface of claim 1 wherein event severity is a numerical value entered by the user.

7. (Original) The graphical user interface of claim 1 wherein the fields are implemented a pull-down fields.

8. (Currently Amended) A method for detection of a new service involving host in a network an entity, the method comprises:

retrieving a baseline list of port and/or service protocols used by a host an entity being tracked, the baseline list listing service and/or port protocols used by that host value determined over a baseline period that is of a longer duration than a current period;

retrieving a current list of service and/or port protocols for the current period used by for the host entity being tracked; and

determining whether there is a difference in the port protocols, by having finding a protocol that was in a the current list but was not in the baseline list; and if there is a difference; indicating a new service involving the tracked host entity.

9. (Currently Amended) The method of claim 8 further comprising:
determining if the host entity is providing or using the new service.

10. (Currently Amended) The method of claim 9 further comprising:
determining whether a rule specified to issue an alert if the host entity is providing or using the new service; and
determining if the host entity is providing or using the new service; and if both determining actions match
issuing the alert.

11. (Currently Amended) The method of claim 9 10 further comprising:
retrieving a value corresponding to the alert severity level set for violation of the rule.

12. (Currently Amended) The method of claim 8 wherein a property of the host being tracked is that the entity host is at least one of a specific host, any host in a specific role, any host in a specific segment, or any host.

13. (Currently Amended) The method of claim 8 wherein the extent of the determining comparison is configured to for that host, in its role, in its segment or anywhere in the network.

14. (Original) The method of claim 8 wherein the baseline and current lists of protocols are provided from data in a connection table.

15. (Currently Amended) A computer program product residing on a computer readable medium for detection of new services in a network, the computer program product comprising instructions for causing a computer to:

retrieve a baseline list of port and/or service protocols used by a host an entity being tracked, the baseline list listing service and/or port protocols used by that host value determined over a baseline period that is of a longer duration than a current period;

retrieve a current list of service and/or port protocols for the current period used by the host for the entity being tracked; and

determine whether there is a difference in the port protocols, by having identifying a protocol that was in the current list but was not in the baseline list; and if there is a difference; indicate a new service involving the tracked host entity.

16. (Currently Amended) The computer program product of claim 15 further comprising instructions to:

determine if the host entity is providing or using the new service.

17. (Currently Amended) The computer program product of claim 15 further comprising instructions to:

determine whether a rule specifies to issue an alert if the host entity is providing or using the new service; and

issue the alert if the rule is violated.

18. (Original) The computer program product of claim 15 wherein instructions to indicate further comprise instructions to:

issue an alert if the new service is detected.

19. (Currently Amended) The computer program product of claim ~~15~~ 17 further comprising instructions to:

retrieve a value corresponding to the alert severity level set for violation of the rule.

20. (Currently Amended) The computer program product of claim 15 wherein a property of the host being track is that the entity host is at least one of a specific host, any host in a specific role, any host in a specific segment, or any host.

21. (Currently Amended) The computer program product of claim 15 wherein the extent of the comparison determining is configured to for that host, in its role, in its segment or anywhere in the network.

22. (Original) The computer program product of claim 15 further comprising instructions to:

access a connection table to provide data for the baseline and current lists of protocols.